

REMARKS/ARGUMENTS

Claims 1-23 and 26-31 are pending. Claims 1, 2, 9, 12, 13, 16, 17, 23, 26, 27, and 30 have been amended. Claims 24 and 25 have been canceled. No new matter has been added.

The drawings were objected to for failing to comply with 37 C.F.R. § 1.84(p)(5). A new Fig. 1 including numerals 133 and 135 has been submitted in response to the objection. The specification, on pages 7 and 8, have been amended to include new paragraphs that more fully describe Figs. 4, 5, 6, 7, and 8. Since these paragraphs are based on the figures that were originally submitted, Applicants believe the present amendment does not add any new matter.

The disclosure was objected to for informalities. The second paragraph on page 6 has been amended in response to the objection.

Claims 4-8 and 25 were objected to for informalities. The Examiner stated that claims 4-8 have been numbered improperly, stating that if claims are canceled, the remaining new claims must not be renumbered. Applicants note that no claims has been canceled prior to the present amendment and are not sure as to the Examiner's ground for the objection on claims 4-8. Claim 25, on the other hand, has been canceled since many of the features therein are included in claim 26.

Claims 1, 12, 16, 17, and 25-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohran in view of Yanai et al. Applicants respectfully traverse the rejection. The claimed invention relates to data transfer between a local disk system and a remote disk system. A user may select whether or not the data transferred in encrypted form is to be stored in the encrypted form or in decrypted form. The claimed invention also permits a user to change the encryption/decryption key without stopping the I/O operation from the host computer and further avoids mis-decryption of the data at the remote disk system, i.e., by using an inappropriate key (see, page 6:22 to page 7:9).

Regarding claim 1, the Examiner asserted that Ohran at col. 11:40-43 discloses "determining whether the data is to be stored in an encrypted form." This section of Ohran merely states that the key that has been used to encrypt is used to decrypt some or all of the information that has been transferred between the systems. It does not state that it is possible to

store the received data in the encrypted form or in decrypted form, in the manner recited. In the claimed invention, the received data may be stored without decrypting them, as recited in the claim (see also, page 8, lines 8-10 of the specification).

In addition, Ohran relates to data transmission between servers, whereas the claimed invention relates to data transmission between storage devices (i.e., disk systems). For example, Ohran states that "primary system" is "a network server computer connected to a computer network. Primary system 12 may also be a stand-alone system. Primary system 12 may also be a backup or standby server of a computer network connected to a primary server (col. 9:13-17)." Ohran further states, "[p]rimary system 12 has attached thereto primary mass storage means for storing a plurality of data blocks in a plurality of storage locations (col. 9:29-31)". Accordingly, the "local disk system" corresponds more closely to the primary mass storage means of Ohran rather than the primary system 12.

Ohran, consequently, does not disclose data transmission between two disk systems, where the local system is "coupled to a host computer to allow the host computer to access data stored in the local disk system." Yanai does not remedy the deficiencies of Ohran. Claim 1 is allowable at least for the reasons set forth above.

Claim 12 relates to a method for changing an encryption key while operating a storage system having a local disk system and a remote disk system. The claim recites, "storing an encryption key in a memory in the local disk system; transmitting the encryption key to the remote disk system and storing it in a memory there; issuing split request from the local disk system to the remote disk system to allow them to operate independently; using a new encryption key to begin storing data in the local disk system after issuing the split request; using a new encryption key to begin storing data in the remote disk system after receiving the split request; and resynchronize the local disk system and the remote disk system." The above method discloses a method of preventing mis-decryption at the remote disk system (see steps 550 and 560 and steps 750 and 760). That is, a new key is used once a request to split the volumes has been received/issued. Neither Ohran nor Yanai, alone or in combination, disclose the above recited features. Claim 12 is allowable at least for these reasons.

Claim 16 recites, "switching encryption to an opposite state from a previous state after splitting the local disk system and remote disk system." Neither Ohran nor Yanai, alone or in combination, disclose this feature. Claim 12 is allowable.

Claim 17 recites, "a communications link coupling the local system to the remote system...wherein the remote disk system determines whether to store the data in either encrypted form or unencrypted form and stores the data in that form in the remote disk system, and notifies the local disk system that the data has been stored." Ohran does not disclose data transfer between disk systems using encryption and decryption methods. Yanai does not remedy this deficiencies of Ohran. In addition, neither references disclose or suggest storing the received data in encrypted or not-encrypted form, as recited in claim 17. Therefore, claim 17 is allowable.

Claim 26 is directed to a system for controlling encryption in a storage system having a local system and a remote system. The claim recites, "a local memory storing an encryption key in the local system; a communications link for transmitting the encryption key to the remote disk system and storing it in a remote memory there; a first computer program for splitting the local system from the remote system to allow them to operate independently; a switch for changing encryption to an opposite state from a previous state after splitting in the local disk system and remote disk system; and a second computer program for re-synchronizing the local system and the remote system." None of the above references disclose or suggest these features. Claim 26 is allowable at least for this reason.

Claim 30 is directed to a storage system. The claim recites, "a local disk system including a plurality of volumes of media for storing data, wherein the local disk system is connected to a host computer; a remote disk system including a plurality of volumes of media also for storing data; a communications link coupling the local disk system to the remote disk system, wherein the local disk system retrieves selected data from one of the volumes on the local system, encrypts that selected data using an encryption key; , and transmits the encrypted selected data to the remote disk system, and wherein the remote disk system decrypts the selected data received from the communications link and stores that selected data in unencrypted form in one of the volumes of media the remote system." As recited, the local disk system performs the encryption and transmits the data to the remote disk system. Ohran does not

disclose these features. In Ohran, the primary system or host performs these functions. Claim 30 is, therefore, allowable at least for these reasons.

Claims 2-8, 18-22, and 31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohran in view of Yanai and further in view of Jacobson. These claims depend from one of the independent claims above and are allowable at least for this reason.

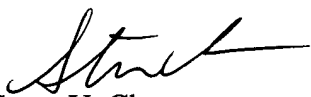
Claims 9-11, 13-15, 23 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohran. These claims depend from one of the independent claims above and are allowable at least for this reason.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,


Steve Y. Cho
Reg. No. 44,612

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
SYC:asb
60199731 v1

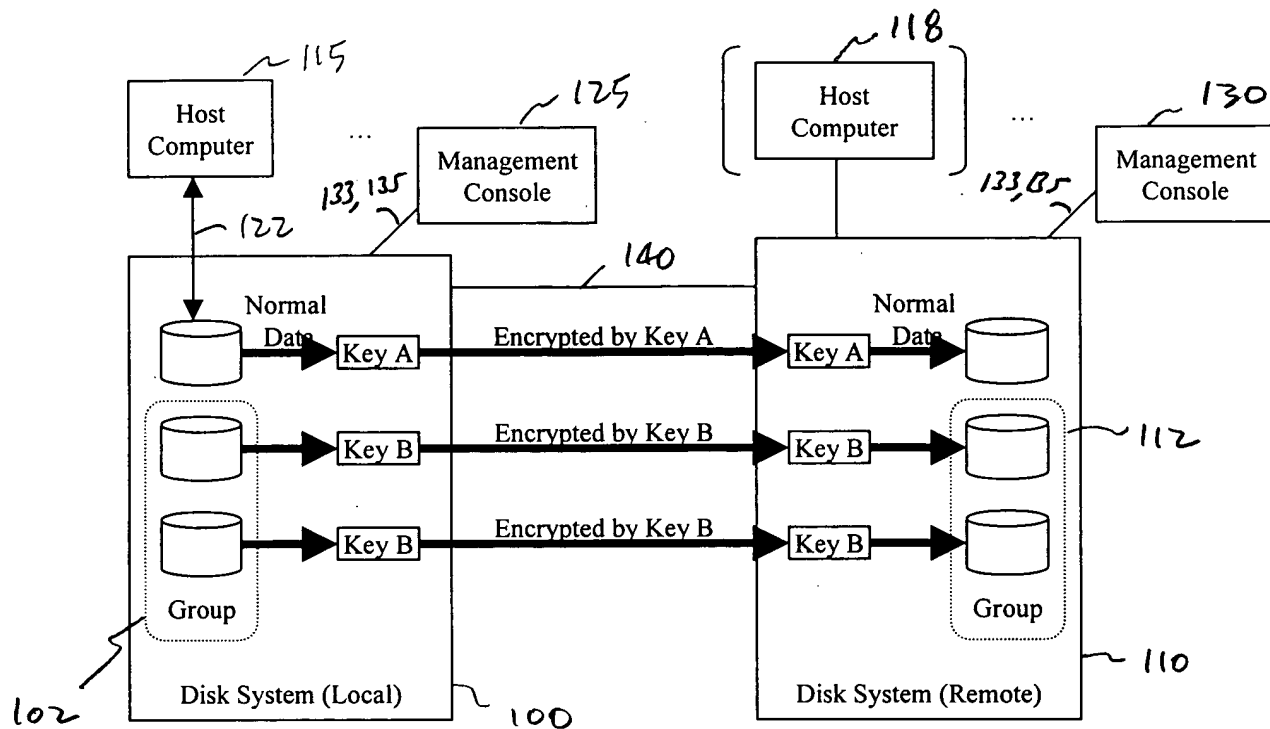


Figure 1. System Configuration

Key	Encryption	Decryption	Volume
0x12345678	YES	YES	158
0x12ab58cf	NO	NO	159
0xaf8329bb	YES	NO	160
...

Local → Remote

Figure 2. Encryption Control Table 200